ACS CYBERSECURITY SERVICES

TABLE OF CONTENTS

Cybersecurity Assessments

vCISO

ThreatID, Custom Assessments, Pen Testing

FEATURES:

- ThreatID using industry-recognized guidelines from The National Institute of Standards and Technology
- Custom assessments available, these can include review of physical environment and endpoints, employee interviews, etc. depending on business needs
- Penetration testing (with automated tools or performed by one of ACS' engineers, depending on business needs)

BUSINESS PROBLEM SOLVED:

Reduce risk of data breaches and loss, regulatory issues, and downtime. It's difficult to be well-protected when you don't understand where your weaknesses are. Our security assessment will determine threats and vulnerabilities, then provide practical, prioritized recommendations for strengthening your security posture in the short and long-term. Identifying current and future threats will allow you to mitigate risk and long-term costs by reducing security incidents that can cost your organization money and reputational damage.

DNS-layer Security

Managed Services
ThreatProtect
vCISO

FEATURES:

- Web filtering by domain or category
- Custom block/allow list of domains
- Cloud app discovery, risk scoring, blocking and activity controls
- Block domains with malware, phishing, botnet or other high-risk items

BUSINESS PROBLEM SOLVED: Protect your company's domain name system (DNS) infrastructure with DNS-layer security that inspects sites at the source and blocks users from visiting websites that are found to be malicious. Avoid spear phishing attacks, user errors like clicking on bad links, or divulging sensitive information on spoofed websites. Without DNS-layer protection, your company's computers will connect to DNS servers and websites regardless of their potential dangers because there is nothing to indicate they may be malicious.

Documentation and Governance

vCISO

FEATURES:

- Framework Assessments
- Policy Assessments
- Planning and documentation for Incident Response, Business Continuity, and Disaster Recovery
- Managed Compliance (SOC2, ISO, NIST, etc.)

BUSINESS PROBLEM SOLVED: Governance and documentation services assist clients in ensuring they achieve maximum compliance and adhere successfully to the requirements of their company, industry, and cyber liability insurance policy. Framework assessments prepare clients to pass their next framework audit or certification, while policy assessments offer thorough review of the client's current security policies to ensure they are effectively covered. Verifying that all security boxes are checked is more vital than ever now that cyber liability insurance requirements have become increasingly stringent.

When the unexpected happens, having a thorough, well-tested plan can be the difference between catastrophic loss and rapid return to business as usual. ACS offers strategic planning and documentation support for Incident Response, Business Continuity, and Disaster Recovery, helping companies develop critical plans and processes to determine the appropriate course of action in case of a ransomware attack, cybersecurity breach, accidental data loss, or natural disaster.

Email Security

Managed Services

FEATURES:

- Defend against phishing and business email compromise
- Secure email domain protection
- Combat ransomware and malware hidden in attachments
- Protect sensitive content in outgoing emails with Data Loss Prevention
- Drop emails with risky links automatically or block access to newly infected sites with real-time URL analysis

BUSINESS PROBLEM SOLVED:
Human error is the leading cause of data breaches. All it takes is one bad email, link or attachment to do major damage. Protect your users' inbound and outbound emails to avoid phishing attacks, ransomware and malware, and keep sensitive information secure.

Endpoint Security

Managed Services

ThreatProtect

FEATURES:

- Anti-malware and anti-virus
- Host-based intrusion detection
- App visibility and control
- Health monitoring
- Endpoint detection and response
- Dynamic file analysis
- Vulnerability identification
- Endpoint isolation
- Mobile device management (MDM)

BUSINESS PROBLEM SOLVED:

Protect your company's physical devices (laptops, desktops, phones, and any device connected to the network) from viruses and malware in real-time. With the rising prevalence of "bring your own device", the ability to securely monitor, manage, and remotely wipe any device is also critical.
Stop threats at the earliest point in time to ensure minimal damage to endpoints and less dxowntime in case of a breach.
Prevent breaches, block malware at the point of entry, and continuously monitor and analyze file and process activity to rapidly detect, contain, and remediate threats that can evade frontline defenses.

Emergency Incident Response

vCISO

FEATURES:

- 24x7 coverage
- Expertise to identify, contain, and eradicate the threat as safely and quickly as possible.

BUSINESS PROBLEM SOLVED:

In the event of a destructive attack, data breach, ransomware demand, or accidental data loss, time is of the essence. ACS steps in by providing cybersecurity engineers to offer around-the-clock emergency response and help clients recover from cybersecurity incidents, return to business as usual, and perform careful post-incident analysis to prevent future incidents.

Firewall

Managed Services

ThreatProtect *(optional)*

FEATURES:

- Intrusion detection and prevention
- Anti-malware and anti-virus protection on network level
- Virtual Private Network (VPN)

BUSINESS PROBLEM SOLVED:

A key component of a layered security approach, firewalls protect your network and information by acting as a chokepoint filtration system for your network traffic. This includes blocking unsolicited incoming network traffic and validating access by assessing network traffic for anything malicious like hackers and malware.

Network Equipment Patching

Managed Services
ThreatProtect

FEATURES:

- Reliable, up-to-date security patches guaranteed
- Patches installed according to the client's business schedule
- Peace of Mind deployment and testing

PROBLEM SOLVED:

Ensure each client's infrastructure is stable and as protected as possible with up-to-date software patches.

Multi-factor Authentication (MFA)

Managed Services
ThreatProtect

FEATURES:

- Streamlined login experience with identity verification in seconds
- Protect any application on any device with second source of validation
- Easy deployment in any environment

PROBLEM SOLVED:

Make it more difficult for cybercriminals to access your data by requiring that the user supply credentials from a different device or channel. A phishing attack may garner a user's credentials, but it won't provide the hacker with a fingerprint or the answer to a personal security question. MFA acts as an added layer of protection.

Note: Cybersecurity insurance providers are increasingly mandating that MFA be in place as a base requirement to receive coverage from a cyberattack.

Security Remediation

vCISO

FEATURES:

- Vulnerability scanning
- Preventative approach to network optimization
- Provides peace of mind knowing remediation is complete

BUSINESS PROBLEM SOLVED:

Identify and remediate vulnerabilities that are of greatest impact to improve the client's security posture. Security remediation also provides staff augmentation and allows overloaded internal IT teams to hand off monitoring and have peace of mind knowing remediation can be counted on.

SoC and SIEM Services

Managed Services

ThreatProtect

FEATURES:

- 24x7 network and event monitoring
- Analyzes and centralizes logs from every network
- Utilizes AI and human oversight to detect and analyze correlations between different types of events
- Anomaly and risk detection
- Network troubleshooting
- Network monitoring and oversight
- Persistent threat detection

BUSINESS PROBLEM SOLVED:

Utilize Security Operations Center (SoC) and SIEM (Security Incident and Event Management) services as a more affordable alternative to a high-cost, comprehensive internal security team.

Cybersecurity threats are constantly evolving. Most internal security teams lack the capacity to investigate each one and monitor endpoints and networks at all times, all while maintaining the other responsibilities of their jobs. Security analysts are also in high demand and command costly salaries. Instead of taking on the risk of turnover and the responsibility of paying and training a team to keep up with ever-changing threats, clients can entrust their security needs to ACS.

Our security engineers are constantly developing their skills and use what they learn from other client's issues to strengthen their security posture. Thanks to our partnership with Arctic Wolf, clients are guaranteed the services of an experienced, knowledgeable team who will be their eyes and ears and monitor their network 24x7.

Unstructured Data Security

vCISO

FEATURES:

- Connects to all systems where data lives (on-prem, cloud, apps, directory, network)
- Permission auditing and monitoring
- Simulate, commit, and automate changes in the environment
- Profile behavior and surface risk insights without human intervention
- Produce a human-readable audit trail for all data access
- Enforce Least Privilege
- Security Analytics & Threat Modeling

BUSINESS PROBLEM SOLVED:

Most companies don't have an accurate, real-time handle on who has access to what data, files, or folders. Keep a constant eye on your data permissions to preve nt unnecessary or unauthorized access. Enforce least privilege and keep track of suspicious patterns of access. Per Varonis, users are 75% less likely to experience a data breach.

User Education

ThreatProtect

vCISO

FEATURES:

- Interactive training
- Phishing, vishing and smishing simulations
- Account takeover monitoring
- Reporting and risk scoring

BUSINESS PROBLEM SOLVED:

Diminish malware infections, data loss, cyber-theft with a security-conscious culture. Increase user awareness and turn your company's employees into its biggest cybersecurity asset.

Virtual CISO

FEATURES:

- Cybersecurity Leadership
- Technical Guidance
- Security Architecture Development
- Technical Assistance
- Risk Management
- Hands-On Guidance and Technical Support
- Incident Response

BUSINESS PROBLEM SOLVED:

With vCISO, top-tier security experts are available to organizations who need security expertise and guidance but may not have the funds to employ a CISO or dedicated network security team. vCISO from ACS protects companies at the same level you would expect from a full-time chief information security officer without the steep investment of executive compensation and their associated benefits package. vCISO increases your company's security posture by acting as an experienced extension of your IT team, allowing for daily checks (with real people, not just software) and constant monitoring. Have peace of mind knowing that your ACS team is keeping track of emerging threats, so you don't have to.

Web Application Firewall (WAF)

FEATURES:

- Hardware and virtual options
- Flexible deployment
- Integration with application delivery controller (ADC) platform
- Daily rule updates
- Cross-site scripting mitigation
- Cookie tampering & data leakage protection
- Custom rule support
- Load balancing

BUSINESS PROBLEM SOLVED:

A WAF acts as a shield between web applications and the internet: filtering, monitoring, and blocking malicious HTTP/S traffic to prevent it from reaching users or web apps. It protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others. WAFs are an increasingly critical part of a holistic, layered cybersecurity approach as businesses expand into new digital initiatives, which can leave new web apps and application programming interfaces (APIs) vulnerable to attacks. WAFs also provide load balancing (distributing network traffic across multiple servers) ensuring applications are always on and improving web server performance.